

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 4, 39 and 48 in accordance with the following:

Claims 1 and 2 (Cancelled)

3. (Withdrawn) A system for managing files, comprising:
sub-file storing means for storing one or a plurality of sub-files related to a main-file;
authentication information creating means for creating sub-file authentication information used to verify the sub-files; and
system file storing means for storing a system file to which the sub-file authentication information is related.

4. (Currently Amended) A system for managing files, comprising:
a main-file storing means for unit storing a main-file in a non-secure area;
an authentication information creating means for unit creating main-file authentication
information to be used to verify the main-file; and
a sub-file storing means for unit storing at least one sub-file to which the main-file authentication information is related in at least one sub-file in a secure area.

5. (Withdrawn) A system for managing files, comprising:
main-file storing means for storing a main-file;
sub-file storing means for storing at least one sub-file to which the main-file authentication information is related;
authentication information creating means for creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and
system file storing means for storing a system file to which the sub-file authentication information is related.

6. (Withdrawn) The system for managing files according to claim 5, wherein said main-file, said sub-files and said system files are stored in a non-secure area usually accessible.

7. (Withdrawn) The system for managing files according to claim 5, wherein said main-file, and said sub-files and said system files are stored in a non-secure area usually accessible and a secure area usually inaccessible, respectively.

8. (Withdrawn) The system for managing files according to claim 5, wherein said main-file and said sub-files, and said system files are stored in a non-secure area usually accessible and a secure area usually inaccessible, respectively.

9. (Withdrawn) The system for managing files according to claim 6, further comprising a computer and a storage unit, wherein the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key, the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from, the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually inaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

10. (Withdrawn) The system for managing files according to claim 7, further comprising a computer and a storage unit, wherein the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing all the access allowing keys; and

file accessing means for sending an access request together with the access allowing key, the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the _access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually inaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

11. (Withdrawn) The system for managing files according to claim 8, further comprising a computer and a storage unit, wherein the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing key; and

file accessing means for sending an access request together with the access allowing key, the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually inaccessible, and the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

12. (Withdrawn) The system for managing files according to claim 9, wherein the reciprocal authenticating means provided in said computer and said file accessing means are implemented by means of hardware.

13. (Withdrawn) The system for managing files according to claim 9, wherein the medium ID is a card ID.

14. (Withdrawn) The system for managing files according to claim 9, wherein the medium ID is a master ID.

15. (Withdrawn) The system for managing files according to claim 9, wherein said authentication information is created for each record of a file.

16. (Withdrawn) The system for managing files according to claim 10, wherein said authentication information is created for each record of a file.

17. (Withdrawn) The system for managing files according to claim 11, wherein said authentication information is created for each record of a file.

18. (Withdrawn) A system for managing files, comprising:
sub-file reading means for reading one or a plurality of sub-files related to a main-file;
authentication information creating means for creating sub-file authentication information from sub-files read by the sub-file reading means;

system file reading means for reading sub-file authentication information from a system file related to the sub-file; and

authentication information comparing means for comparing the sub-file authentication information created by the authentication information creating means with the sub-file authentication information read by the system file reading means.

19. (Withdrawn) A system for managing files, comprising:

main-file reading means for reading a main-file;

authentication information creating means for creating main-file authentication information from a main-file read by the main-file reading means;

sub-file reading means for reading, main-file authentication information from sub-files related to the main-file; and

authentication information comparing means for comparing the main-file authentication information created by the authentication information creating means with the main-file authentication information read by the sub-file reading means.

20. (Withdrawn) A system for managing files, comprising:

main-file reading means for reading a main-file;

sub-file reading means for reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

system file reading means for reading sub-file authentication information from a system file related to the sub-file;

authentication information creating means for creating main-file authentication information from a main-file read by the main-file reading means and creating sub-file authentication information from sub-files read by the sub-file reading means; and

an authentication information comparing means for comparing the main-file authentication information created by the authentication information creating means with the main-file authentication information read by the sub-file reading means and comparing the sub-file authentication information created by the authentication information creating means with the sub-file authentication information read by the system file reading means.

21. (Withdrawn) The system for managing files according to claim 20, wherein said main-file, said sub-files and said system file are stored in a non-secure area usually accessible.

22. (Withdrawn) The system for managing files according to claim 20, wherein said main-file, and said sub-files and said. system file are stored in a non-secure area usually accessible and a secure area usually inaccessible, respectively.

23. (Withdrawn) The system for managing files according to claim 20, wherein said main-file and said sub-files, and said system file are stored in a non-secure area usually accessible and a secure area usually inaccessible, respectively.

24. (Withdrawn) The system for managing files according to claim 21, further comprising a computer and a storage unit, wherein
the computer comprises
reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing keys; and
file accessing means for sending an access request together with the access allowing key, the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and
access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same;
and

secure area accessing means for accessing a secure area usually inaccessible, and
the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

25. (Withdrawn) The system for managing files according to claim 22, further comprising a computer and a storage unit, wherein the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing key; and

file accessing means for sending an access request together with the access allowing key, the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually inaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

26. (Withdrawn) The system for managing files according to claim 23, further comprising a computer and a storage unit, wherein the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing all the access allowing keys; and

file accessing means for sending an access

request together with the access allowing key, the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access-allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least

one access allowing key stored in the access allowing key group storing means, are the same;
and

secure area accessing means for accessing a secure area usually inaccessible, and
the authentication information creating means reads a medium ID peculiar to the medium
stored in the secure area, and uses the medium ID to create the main-file authentication
information and the sub-file authentication information after the computer and the storage unit
are reciprocally authenticated.

27. (Withdrawn) The system for managing files according to claim 24, wherein the
reciprocal authenticating means provided in said computer and said file accessing means are
implemented by means of hardware.

28. (Withdrawn) The system for managing files according to claim 24, wherein the
medium ID is a card ID.

29. (Withdrawn) The system for managing files according to claim 24, wherein the
medium ID is a master ID.

30. (Withdrawn) The system for managing files according to claim 24, wherein said
authentication information is created for each record of a file.

Claims 31 and 32 (Canceled)

33. (Withdrawn) The system for managing files according to claim 9, wherein
authentication information is created using one, two or all of said medium ID, said card ID and
said master ID.

34. (Withdrawn) The system for managing files according to claim 24, wherein
authentication information is created using one, two or all of said medium ID, said card ID and
said master ID.

Claims 35-37 (Cancelled)

38. (Withdrawn) A method of managing files, comprising the steps of:

storing one or a plurality of sub-files related to a main-file;
creating sub-file authentication information used to verify the sub-files; and
storing a system file to which the sub-file authentication information is related.

39. (Currently Amended) A method of managing files, comprising the steps of:
storing a main-file in a non-secure area;
creating main-file authentication information to be used to verify the main-file; and
storing at least one sub-file to which the main-file authentication information is related in
at least one sub-file in a secure area.

40. (Withdrawn) A method of managing files, comprising the steps of:
storing a main-file;
storing at least one sub-file to which the main-file authentication information is related;
creating main-file authentication information to be used to verify the main- file/sub-file
authentication information to be used to verify the sub-files; and
storing a system file to which the sub-file authentication information is related.

41. (Withdrawn) A method of managing files, comprising the steps of:
reading one or a plurality of sub-files related to a main-file;
creating sub-file authentication information from sub-files;
reading sub-file authentication information from a system file related to the sub-file; and
comparing the sub-file authentication information from the sub-files with the sub-file
authentication information from the system file.

42. (Withdrawn) A method of managing files, comprising the steps of:
reading a main-file;
creating main-file authentication information from the main-file;
reading main- le authentication information from sub-files related to the main-file; and
comparing the main-file authentication information from the main-file with the main-file
authentication information from the sub-file.

43. (Withdrawn) A method of managing files, comprising the steps of:
reading a main-file;

reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file; reading sub-file authentication information from a system file related to the sub-file;

creating main-file authentication information from a main-file and creating sub-file authentication information from sub-files; and

comparing the main-file authentication information from the sub-file with the main-file authentication information from the main-file and comparing the sub-file authentication information from the system file with the sub-file authentication information from the sub-file.

Claims 44-46 (Cancelled)

47. (Withdrawn) A computer readable storage medium having a recorded file management program for enabling a computer to execute:

sub-file storing step of storing one or a plurality of sub-files related to a main-file; authentication information creating step of creating sub-file authentication information used to verify the sub-files; and

system file storing step of storing a system file to which the sub-file authentication information is related.

48. (Currently Amended) A computer readable ~~storage medium having encoded with a~~ recorded file management computer program, which when executed causes for enabling a computer to execute the method comprising:

~~main-file storing step of storing a main-file in a non-secure area;~~
~~authentication information creating step of creating main-file authentication information to~~ be used to verify the main-file; and

~~sub-file storing step of storing at least one sub-file to which the main-file authentication~~ information is related in at least one sub-file in a secure area.

49. (Withdrawn) A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file storing step of storing a main-file;
sub-file storing step of storing at least one sub-file to which the main-file authentication information is related;

authentication information creating step of creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

system file storing step of storing a system file to which the sub-file authentication information is related.

50. (Withdrawn) A computer readable storage medium having a recorded file management program for enabling a computer to execute:

sub-file reading step of reading one or a plurality of sub-files related to a main-file; authentication information creating step of creating sub-file authentication information from sub-files;

system file reading step of reading sub-file authentication information from a system file related to the sub-file; and

authentication information comparing' step of comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the system file.

51. (Withdrawn) A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

authentication information creating step of creating main-file authentication information from a main-file;

sub-file reading step of reading main-file authentication information from sub-files related to the main-file; and

authentication information comparing step of comparing the main-file authentication information from the main-file with the main-file authentication information from the sub-file.

52. (Withdrawn) A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

sub-file reading step of reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

system file reading step of reading sub-file authentication information from a system file related to the sub-file;

Serial No. 09/985,677

authentication information creating step of creating main-file authentication information from a main-file and creating sub-file authentication information from sub-files; and

authentication information comparing step of comparing the main-file authentication information from the sub-file with the main-file authentication information from the main-file and comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the main-file.

Claims 53 and 54 (Cancelled)